Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A processing device, comprising:

an input interface for receiving data units containing header information of respective packets;

a first module configurable to perform packet filtering based on the received data units;

a second module configurable to perform traffic analysis based on the received data units;

a third module configurable to perform load balancing based on the received data units; and

a fourth module configurable to perform route lookups based on the received data units.

2. (currently amended) The processing device of claim 1, wherein the processing device is implemented as an Application Specification Integrated Circuit (ASIC).

3. (currently amended) The processing device of claim 2, wherein the traffic analysis performed by the second module includes at least one of sampling, logging, [[and]] or counting.

4. (new) The processing device of claim 1, the header information comprising at least one of a source Internet protocol (IP) address, a destination IP address, an IP type, a source port, a destination port, a differentiated service (DiffServ) byte, an IP fragmentation offset field,

an IP fragmentation control field, or a transmission control protocol (TCP) control bit, and wherein the first module is configured to perform the packet filtering based on the header information.

5. (new) The processing device of claim 1, wherein the first module includes a user-configured filter rule.

6. (new) The processing device of claim 5, wherein when a packet matches the filter rule, the first module is configured to:

accept the packet;

discard the packet; or

reject the packet and transmit an Internet control message protocol (ICMP) message.

7. (new) The processing device of claim 5, the packet filtering performed by the first module comprising accepting a packet that is not explicitly rejected based on the filter rule.

8. (new) The processing device of claim 5, wherein when a packet matches the filter rule, the first module is configured to mark the packet for sampling by setting a bit in a packet notification.

9. (new) The processing device of claim 8, wherein when the packet has been marked for sampling, the second module generates a random number, the second module being

configured to sample the marked packet when the random number is less than a predetermined threshold.

10. (new) The processing device of claim 8, the second module being configure to write the header information associated with the sampled packet to a routing engine of the processing device.

11. (new) The processing device of claim 1, the second module being configured to monitor:

all logical interfaces associated with the processing device;

designated logical interfaces associated with the processing device;

designated protocols;

a range of addresses; or

individual addresses.

12. (new) The processing device of claim 3, wherein the packet performed by the second module may be used to determine respective destinations of the packets, a volume of the packets, and respective contents of the packets.

13. (new) The processing device of claim 5, wherein when a packet matches the filter rule, the second module is configured to log the packet, a log entry associated with the logged packet being accessible for display by using a command-line interface associated with the

processing device, the log entry including at least one of a log time, an input circuit, a protocol type, a source address, or the destination address.

14. (new) The processing device of claim 3, the second module being configured to perform the sampling, logging, or counting at a speed of about OC-192c/STM-64.

15. (new) The processing device of claim 1, wherein the packet filtering performed by the first module comprises performing source address verification to prevent source address spoofing of a network operation center (NOC) system.

16. (new) The processing device of claim 1, the processing device further comprising a loopback interface, wherein the first module is associated with the loopback interface.

17. (new) The processing device of claim 1, the load balancing performed by the third module comprising forwarding packets received from a designated source port or a designated source address to a designated destination port or a designated destination address.

18. (new) The processing device of claim 17, the forwarding of the packets from the designated source port or the designated source address to the designated destination port or the designated destination address maintains an order and a travel path for a TCP session associated with the forwarded packets.

19. (new) The processing device of claim 1, the load balancing performed by the third module comprising:

accepting a packet when the packet is determined to be in-profile;

dropping the packet when the packet is determined to be out-of-profile; or

accepting the packet when the packet is determined to be out-of-profile and marking the accepted packet as out-of-profile.

20. (new) The processing device of claim 19, a first drop precedence being assigned to the in-profile accepted packet, and a second drop precedence being assigned to the out-of-profile accepted packet.

21. (new) The processing device of claim 20, the third module being configured to use a random early detection (RED) algorithm for queue management of the accepted packets based on the first drop precedence and the second drop precedence.

22. (new) The processing device of claim 1, the load balancing performed by the third module comprising assigning respective policing equivalence classes (PECs) to the packets.

23. (new) The processing device of claim 21, the third module being configured to determine an average bandwidth and a maximum burst associated with each PEC.

24. (new) A method of forwarding data packets using an ASIC-based processor, comprising:

receiving a packet including a header;

filtering the received packet based on the header to accept or reject the received packet;

performing traffic analysis on the accepted packet;

performing a route lookup for the accepted packet; and

forwarding the accepted packet based on the route lookup.

25. (new) The method of claim 24, further comprising:

writing a filter rule into the ASIC-based processor prior to the filtering the received packet.

26. (new) The method of claim 25, the filtering comprising accepting the received packet when the filter rule does not explicitly reject the received packet.

27. (new) The method of claim 24, wherein the traffic analysis comprises randomized sampling based on a user-configurable sampling rate.

28. (new) The method of claim 27, wherein the user-configurable sampling rate is defined as one divided by a user-specified integer, the method further comprising:

generating a random number;

comparing the user-configurable sampling rate to the generated random number to form a resulting value; and

performing the sampling when the resulting value is less than the user-configurable sampling rate.

29. (new) An ASIC-based filter for use in a router, comprising:

means for downloading a user-configured filter rule;

means for applying the filter rule to a packet received by the router;

means for accepting the packet when the packet is not explicitly rejected by the filter rule; and

means for determining whether the packet is to be further processed by the router based on a result of the applying the filter rule, the ASIC-based filter being configured to perform independently of other processes being performed by the router.

30. (new) The ASIC-based filter of claim 30, further comprising:

means for discarding the packet that arrives on an inbound circuit when the packet contains a spoofed NOC source address.